FIG. 1

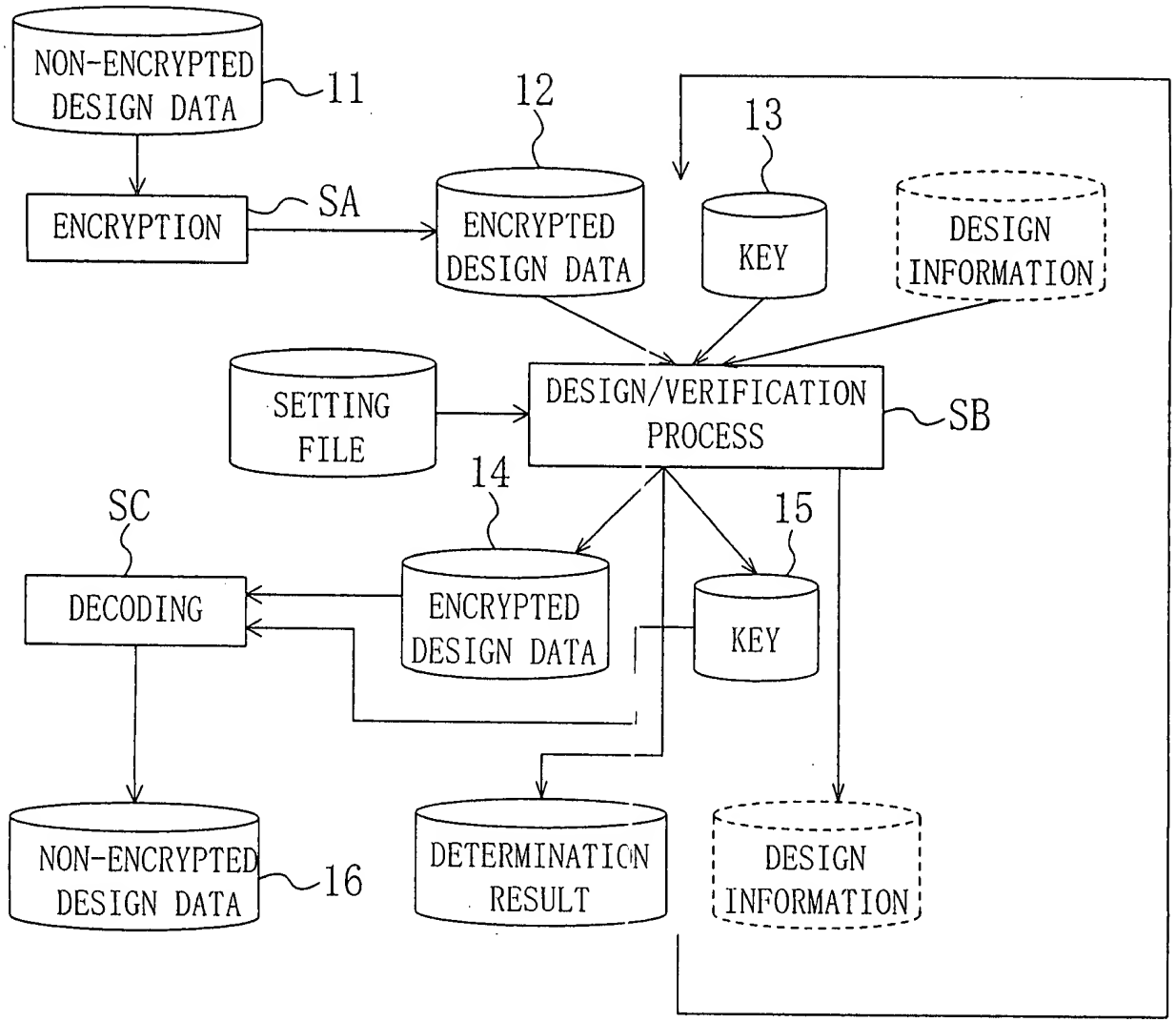

NON-ENCRYPTED DESIGN DATA
11
12
13
ENCRYPTION
SA
ENCRYPTED DESIGN DATA
KEY
DESIGN INFORMATION
SETTING FILE
DESIGN/VERIFICATION PROCESS
SB
14
SC
15
DECODING
ENCRYPTED DESIGN DATA
KEY
NON-ENCRYPTED DESIGN DATA
16
DETERMINATION RESULT
DESIGN INFORMATION

FIG. 2A

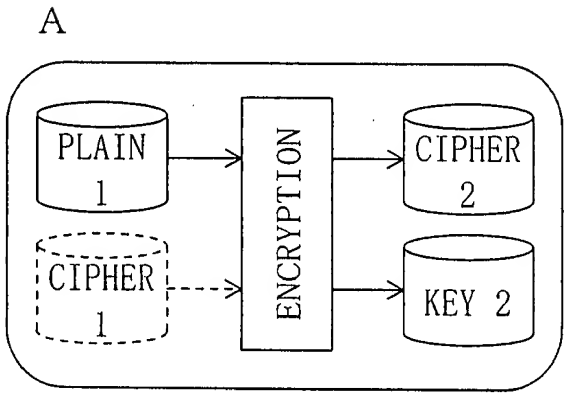



FIG. 2B

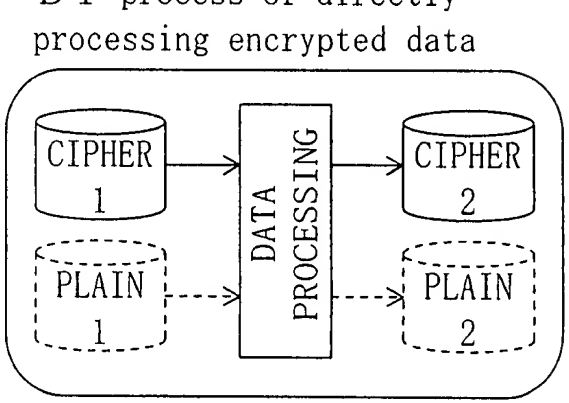



FIG. 2C

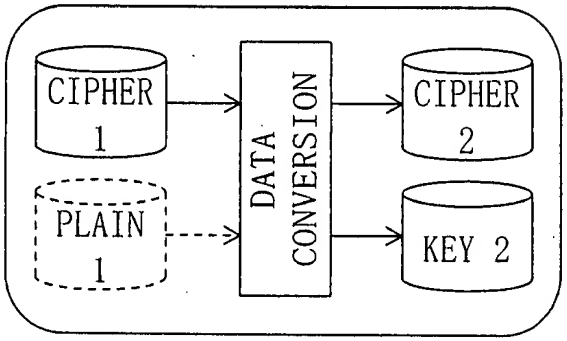
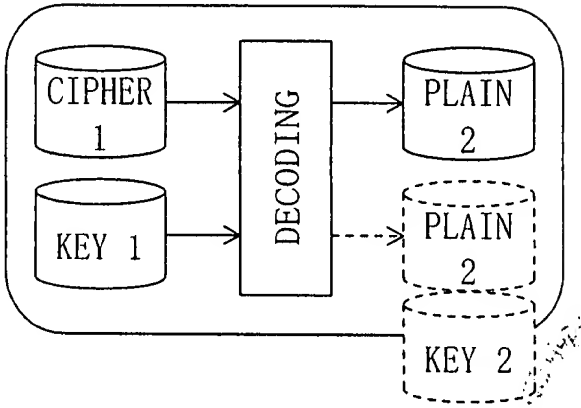



FIG. 2D



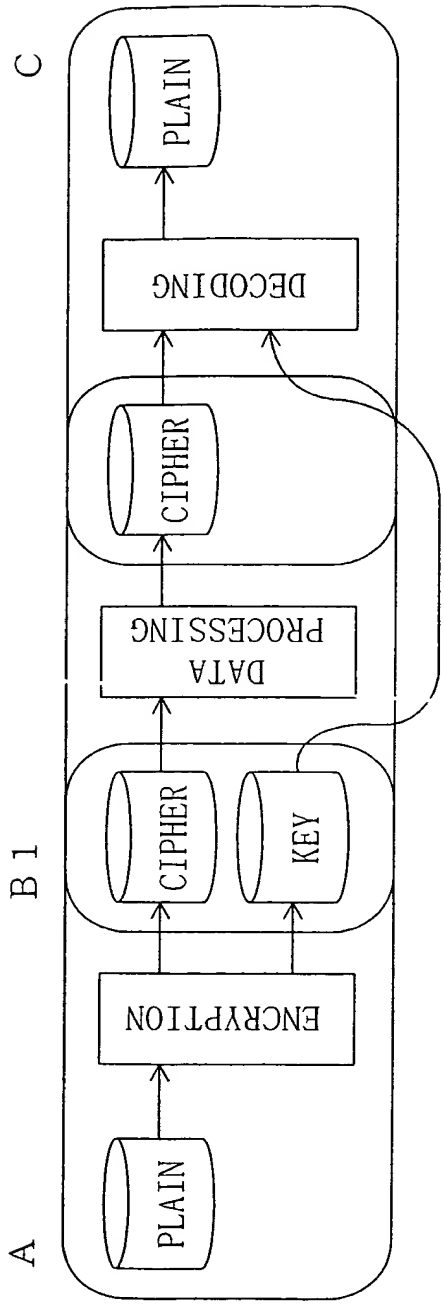

A
B 1
C
PLAIN
ENCRYPTION
CIPHER
KEY
DATA PROCESSING
CIPHER
DECODING
PLAIN

FIG. 3A

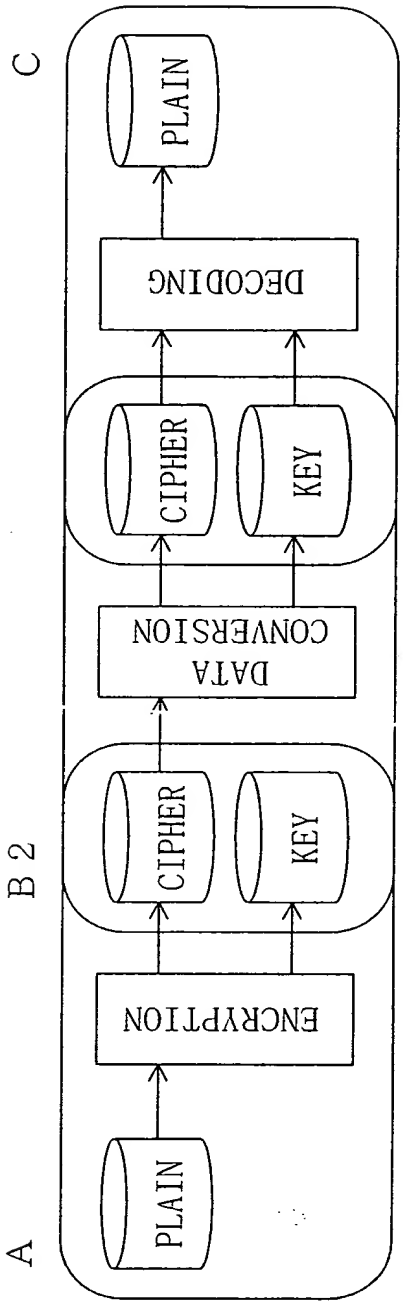

A
B 2
C
PLAIN
ENCRYPTION
CIPHER
KEY
DATA CONVERSION
CIPHER
KEY
DECODING
PLAIN

FIG. 3B

FIG. 4

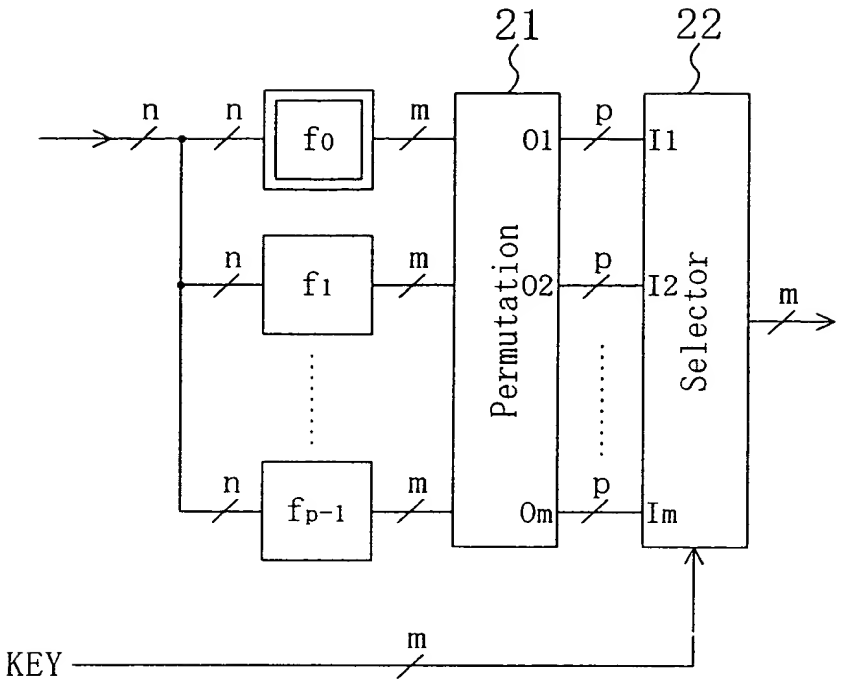

21
22
n
n
f0
m
01
p
I1
n
f1
m
02
I2
m
Permutation
Selector
n
fp-1
m
Om
p
Im
KEY
m

FIG. 5A
ORIGINAL CIRCUIT
$f_0$

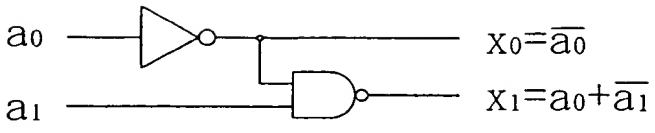



FIG. 5B
DUMMY CIRCUIT
$f_1$

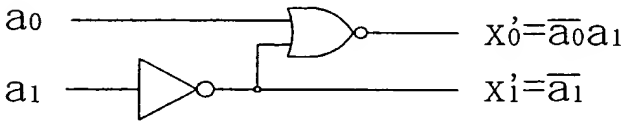



FIG. 5C

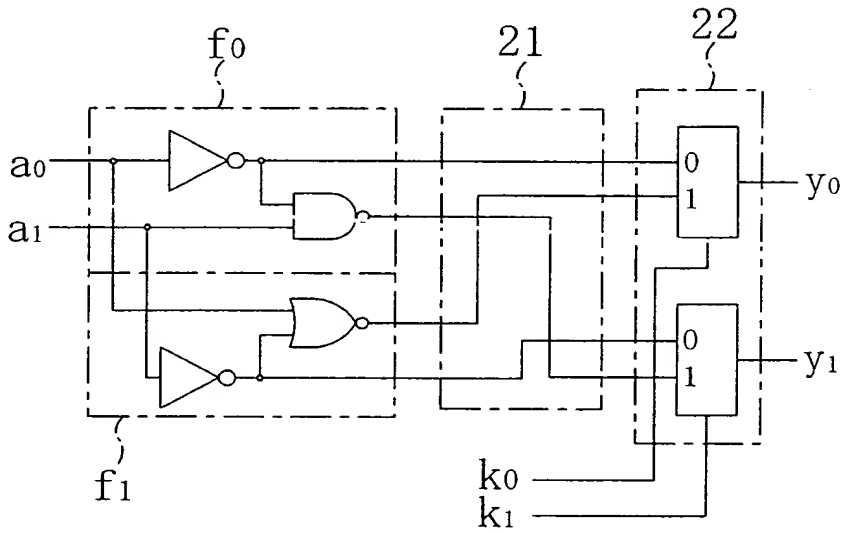
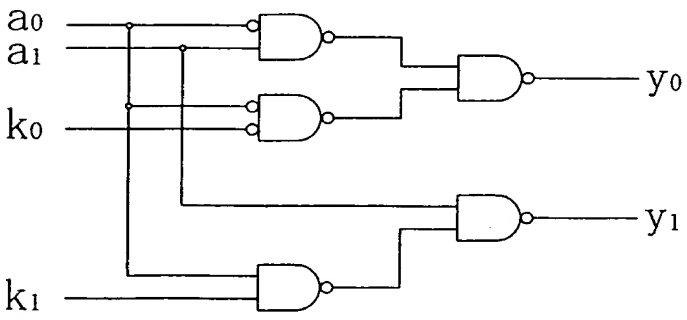



FIG. 5D




KEY=(0, 1)

FIG. 6

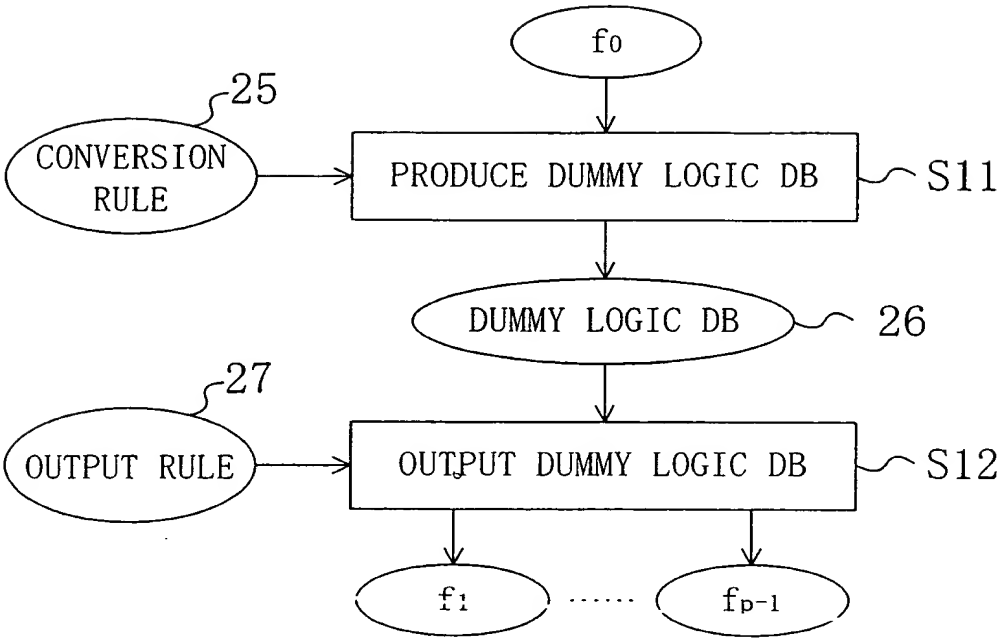

f0
25
CONVERSION RULE
PRODUCE DUMMY LOGIC DB
S11
DUMMY LOGIC DB
26
27
OUTPUT RULE
OUTPUT DUMMY LOGIC DB
S12
f1
fp-1

FIG. 7B

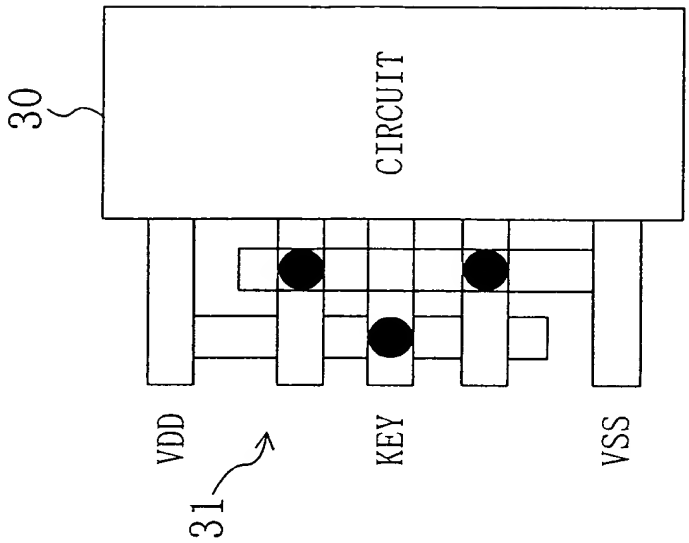



FIG. 7A

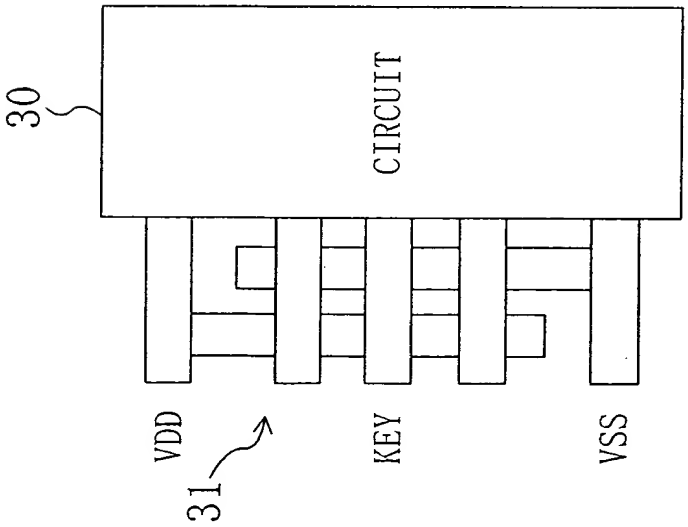


FIG. 8

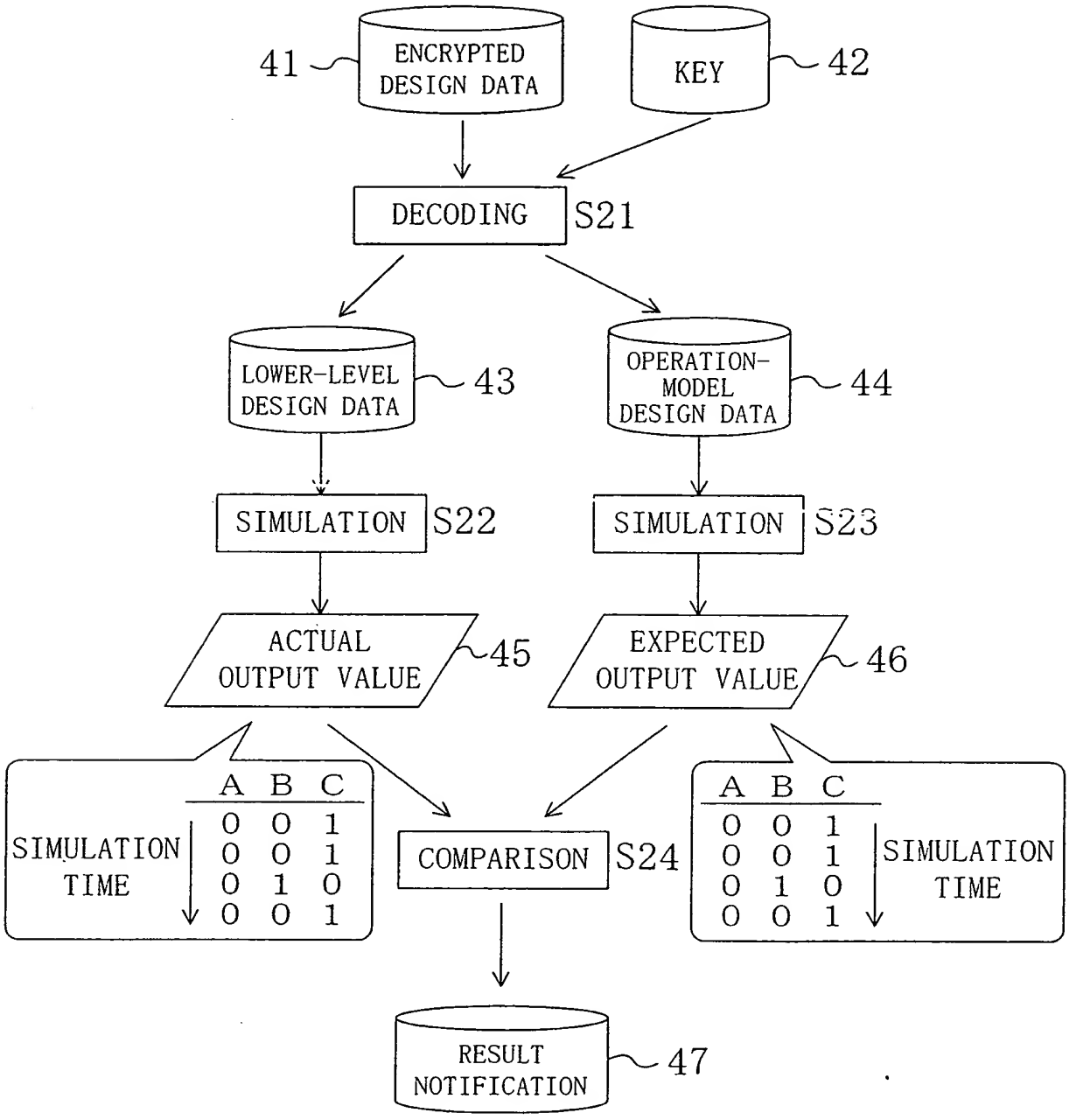

41
ENCRYPTED DESIGN DATA
KEY
42
DECODING
S21
LOWER-LEVEL DESIGN DATA
43
OPERATION-MODEL DESIGN DATA
44
SIMULATION
S22
SIMULATION
S23
ACTUAL OUTPUT VALUE
45
EXPECTED OUTPUT VALUE
46
A B C
0 0 1
0 0 1
0 1 0
0 0 1
SIMULATION TIME
COMPARISON
S24
A B C
0 0 1
0 0 1
0 1 0
0 0 1
SIMULATION TIME
RESULT NOTIFICATION
47

FIG. 9

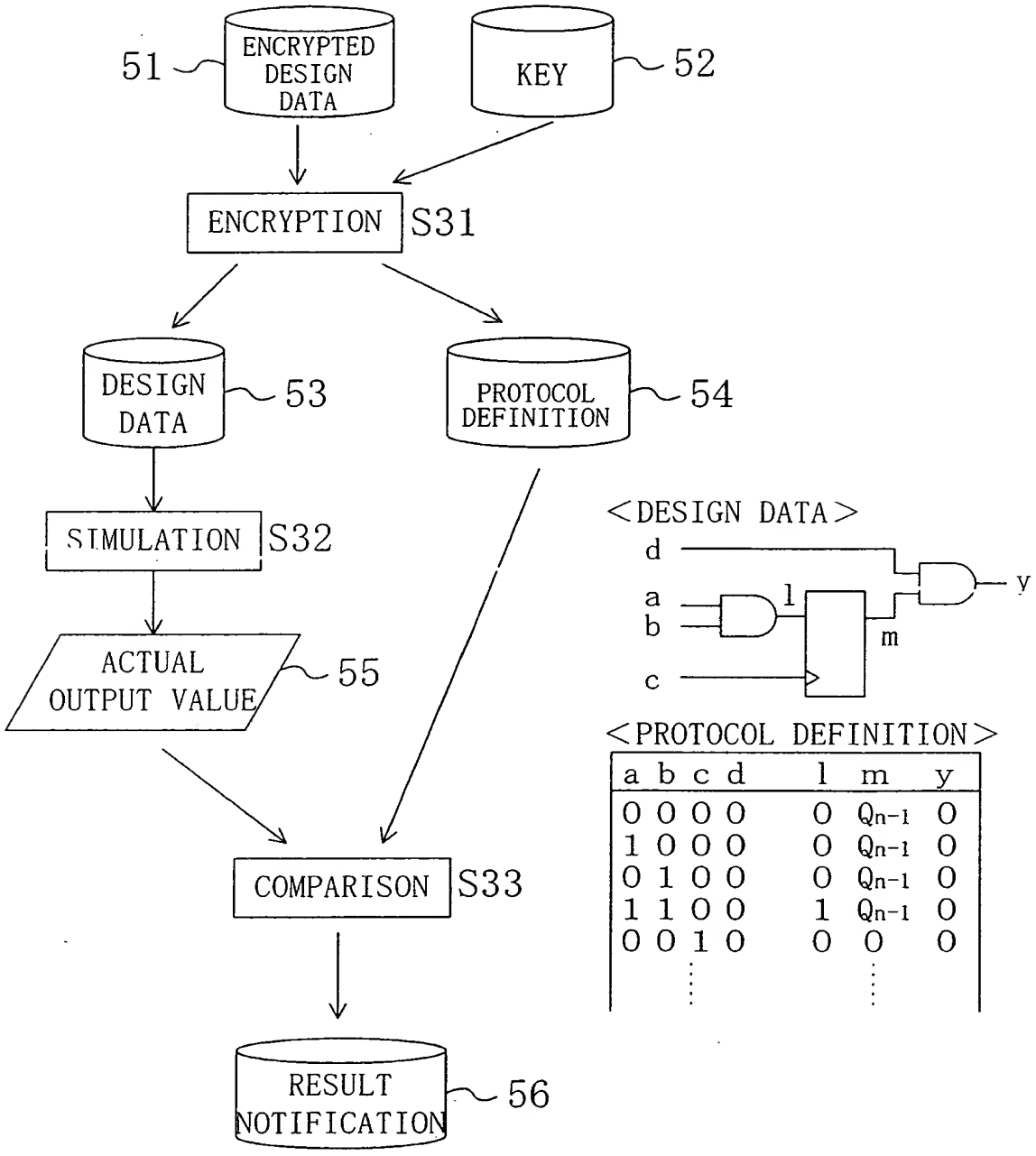

51
ENCRYPTED DESIGN DATA
KEY
52
ENCRYPTION
S31
DESIGN DATA
53
PROTOCOL DEFINITION
54
SIMULATION
S32
ACTUAL OUTPUT VALUE
55
COMPARISON
S33
RESULT NOTIFICATION
56
<DESIGN DATA>
d
a
b
c
l
m
y
<PROTOCOL DEFINITION>
a b c d l m y
0 0 0 0 0 Qn-1 0
1 0 0 0 0 Qn-1 0
0 1 0 0 0 Qn-1 0
1 1 0 0 1 Qn-1 0
0 0 1 0 0 0 0

FIG. 10

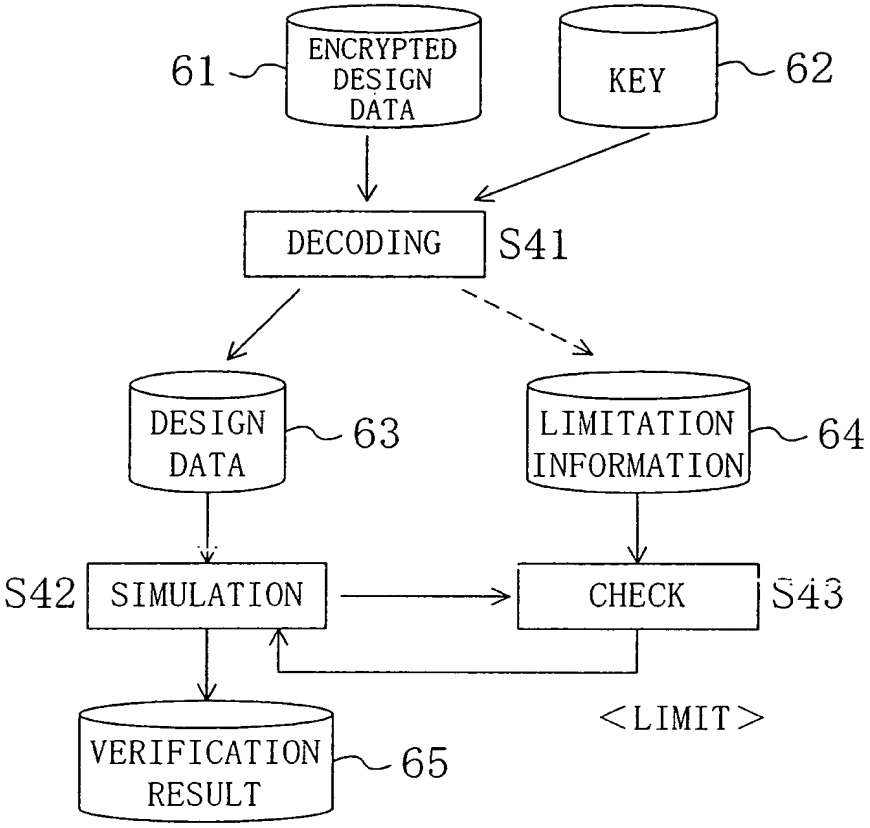

61
ENCRYPTED DESIGN DATA
KEY
62
DECODING
S41
DESIGN DATA
63
LIMITATION INFORMATION
64
S42
SIMULATION
CHECK
S43
<LIMIT>
VERIFICATION RESULT
65

FIG. 11A

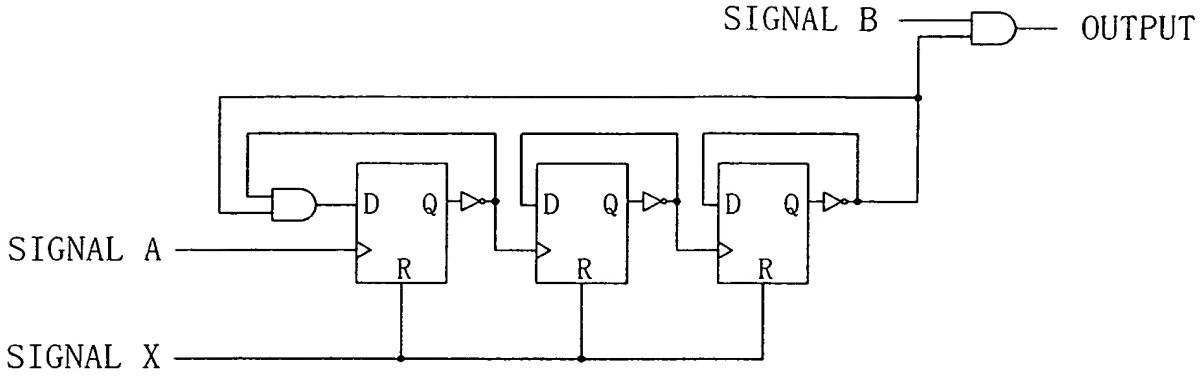



FIG. 11B

| X | NUMBER OF TIMES A CHANGES | B | OUTPUT | |
|---|---|---|---|---|
| 0 | 1 | 0 | 0 | OK |
| | | 1 | 1 | |
| 0 | 2 | 0 | 0 | OK |
| | ⋮ | 1 | 1 | |
| | | | ⋮ | |
| 0 | 7 | 0 | 0 | OK |
| | | 1 | 1 | |
| 0 | 8 | 0 | 0 | NG |
| | | 1 | 0 | |
| 0 | 9 | 0 | 0 | NG |
| | ⋮ | 1 | 0 | |
| | | | ⋮ | |

FIG. 12A

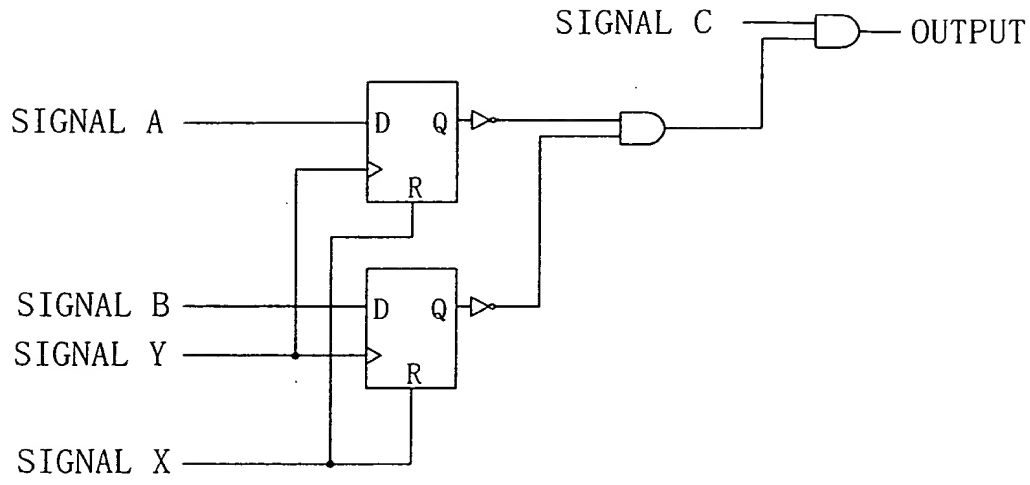



FIG. 12B

| X | Y | A | B | C | OUTPUT | |
|---|---|---|---|---|---|---|
| 0 | ↑ | 0 | 0 | 0 | 0 | OK |
| | | 0 | 0 | 1 | 1 | |
| | | 0 | 1 | 0 | 0 | NG |
| | | 0 | 1 | 1 | 0 | |
| | | 1 | 0 | 0 | 0 | |
| | | 1 | 0 | 1 | 0 | |
| | | 1 | 1 | 0 | 0 | |
| | | 1 | 1 | 1 | 0 | |

FIG. 13

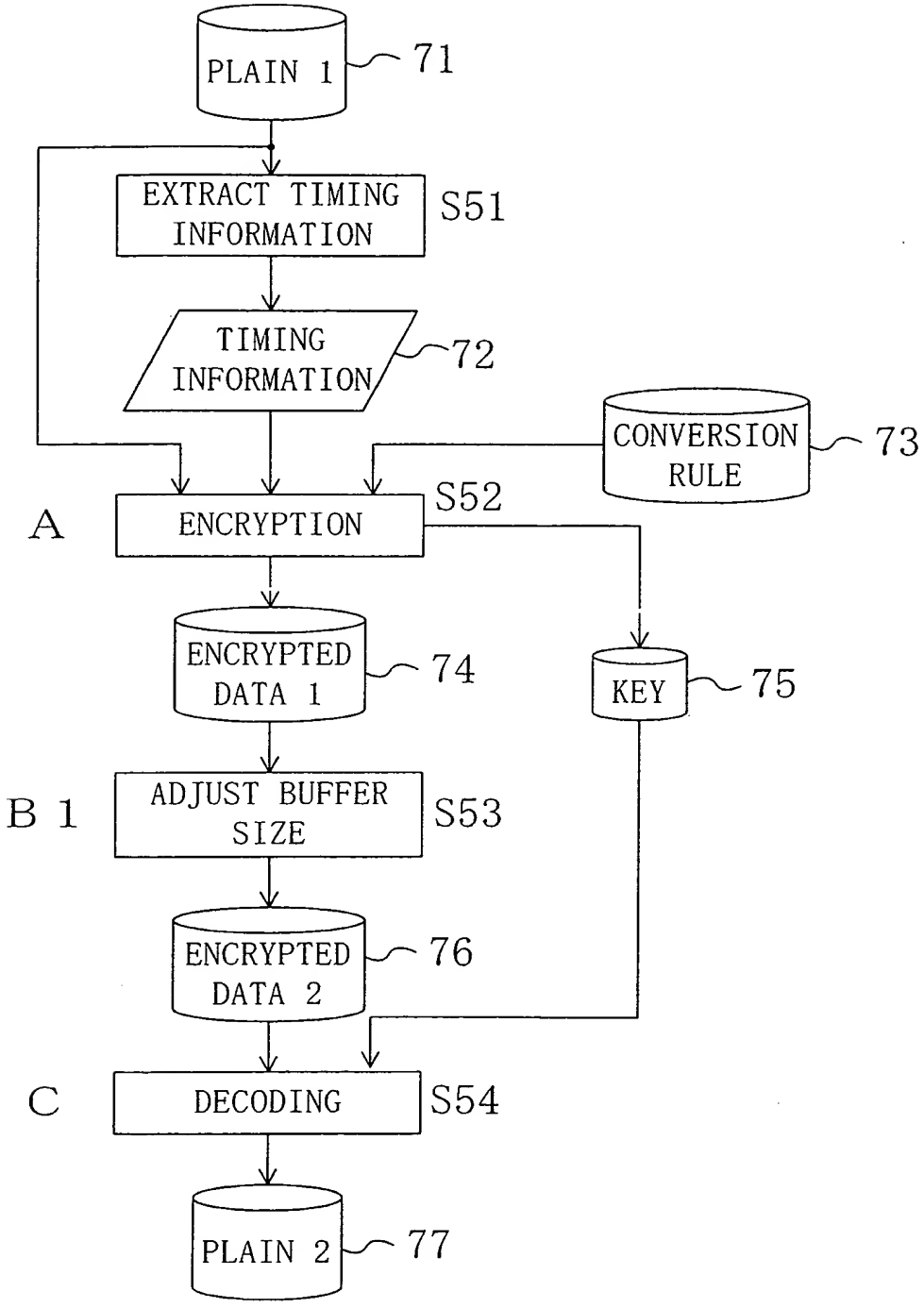

PLAIN 1
71
EXTRACT TIMING INFORMATION
S51
TIMING INFORMATION
72
CONVERSION RULE
73
A
ENCRYPTION
S52
ENCRYPTED DATA 1
74
KEY
75
B 1
ADJUST BUFFER SIZE
S53
ENCRYPTED DATA 2
76
C
DECODING
S54
PLAIN 2
77

FIG. 14A

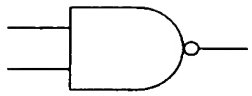


FIG. 14B

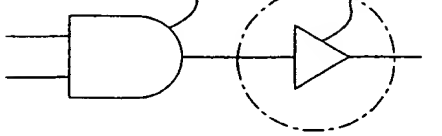



FIG. 14C

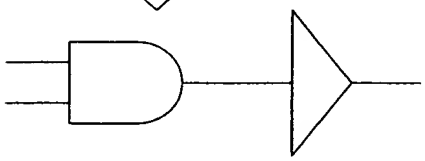


FIG. 14D

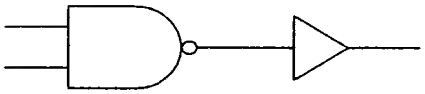
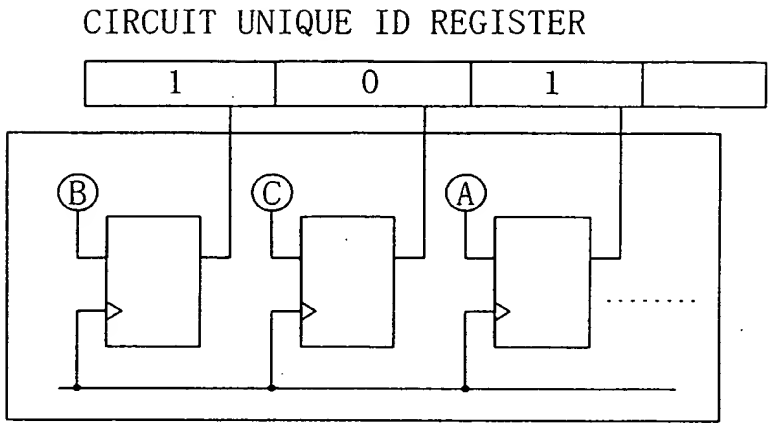


FIG. 15




A = 1
B = 1
C = 0
} UNIQUE PARAMETER

FIG. 16